CLAIMS

1. A method for achieving agreement among n participating network devices to a first agree-value (Y) or a second agree-value (N) in an asynchronous network, the agreement arising out of a series of messages being sent and received by each participating network device, whereby the number t of faulty devices is less than $n/3$, each participating network device performing the following steps:

   a) broadcasting to the participating network devices a pre-vote message comprising a pre-vote variable with a first pre-vote value or a second pre-vote value, and comprising a first signature proving the pre-vote and a second signature justifying the pre-vote variable;

   b) once having received $n - t$ valid of the pre-vote messages with pre-vote variables from the participating network devices, performing a main-vote to obtain a main-vote variable with either a first main-vote value, a second main-vote value, or a third main-vote value, whereby

      - if all $n - t$ pre-vote variables have the first pre-vote value then the first main-vote value is obtained, or
      - if all $n - t$ pre-vote variables have the second pre-vote value then the second main-vote value is obtained, or
      - if the $n - t$ pre-vote variables are different then the third main-vote value is obtained;

   c) broadcasting to the participating network devices a main-vote message comprising the obtained main-vote variable, the first signature and the second signature; and

   d) once having received $n - t$ valid of the main-vote messages, performing a decision,

      - if all $n - t$ main-vote variables have the first main-vote value then deciding for the first agree-value or
      - if all $n - t$ main-vote variables have the second main-vote value then deciding for the second agree-value,

      thereby having achieved the agreement, and helping the other participating network devices to decide; otherwise

   a) broadcasting to the participating network devices a share-value($g^{x_{A,B,C,D}}$) to generate an unpredictable bit $\in$ {Y, N};

b) receiving at least k share-values $(g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D})$ from the participating network devices, where k is a number larger than t, assembling out of those a common value and deriving one bit thereof ; and

c) repeating the steps starting from a), whereby

- if all $n - t$ main-vote variables have the third main-vote value then the binary value is used as the pre-vote variable, or
- if at least one of all $n - t$ main-vote variables has the first main-vote value then the first pre-vote value is used as the pre-vote variable, or
- if at least one of all $n - t$ main-vote variables has the second main-vote value then the second pre-vote value is used as the pre-vote variable.

2. A method for achieving agreement among n participating network devices to a first or second agree-value in an asynchronous network, the agreement arising out of a series of messages being sent and received with a signature by each participating network device, whereby the number t of faulty devices is less than $n/3$, each participating network device performing the following steps:

i) broadcasting to all participating network devices a pre-vote value;

ii) performing a main-vote to amplify majorities if $n - t$ pre-vote values are validly received, and broadcasting to all participating network devices a main-vote value;

iii) deciding for the first or second agree-value based on the received main-vote values, and broadcasting to all participating network devices a share-value to open a cryptographic common coin; and

iv) receiving share-values and assembling out of those a common value, uncovering a bit out of the common value, and repeating the steps starting from i) using the bit as the pre-vote value if the pre-vote values were different.

3. Method according to claim 1, whereby a transaction identifier *TID* is used.

4. Method according to claim 2, whereby a transaction identifier *TID* is used

5. Method according to claim 1, whereby threshold signatures are applied.

6. Method according to claim 2, whereby threshold signatures are applied.

7. Method according to claim 1, whereby a two threshold coin is used, where t is the maximum number of traitors in the asynchronous network and k, with $n > k > t$, the number of participating network devices needed to obtain the two threshold coin.

8. Method according to claim 2, whereby a two threshold coin is used, where t is the maximum number of traitors in the asynchronous network and k, with $n > k > t$, the number of participating network devices needed to obtain the two threshold coin

9. Method according to claim 1, whereby the number t of faulty devices is larger than $n/3$ if all or a part of the faulty devices fail by crashing.

10. Method according to claim 2, whereby the number t of faulty devices is larger than $n/3$ if all or a part of the faulty devices fail by crashing.

11. Method according to claim 1, whereby $t + 1$ participating network devices are used as asynchronous relay stations.

12. Method according to claim 2, whereby $t + 1$ participating network devices are used as asynchronous relay stations.

13. Method according to claim 1, whereby the binary value of the bit is voted by at least one first participating network device if none or not all of the share-values($g^{x_B}, g^{x_C}, g^{x_D}$) have been received from the other participating network devices.

14. Method according to claim 1, whereby at least one first participating network device jumps in a present round of vote even if this participating network device is in a round of vote smaller in number than the present round of vote.

15. Method according to claim 1, whereby at least one of the first signature and the second signature is replaced by a broadcast primitive which guarantees that all the participating network devices receive a sent message or none of them.

16. Method according to claim 1, whereby several rounds are performed in parallel.

17. Method according to claim 1, whereby the number t of faulty devices is extended to a set T of sets comprising participating network devices.

18. Method according to claim 17, whereby the participating network devises show hybrid failures reflecting a different structure of the set T or different thresholds t_i, with $i = 1, 2, \ldots l$.

19. A computer program product comprising program code means for performing the method for achieving agreement among n participating network devices to a first agree-value (Y) or a second agree-value (N) in an asynchronous network, the agreement arising out of a series of messages being sent and received by each participating network device, whereby the number t of faulty devices is less than $n/3$, each participating network device, said method comprising the steps of:

(a) broadcasting to the participating network devices a pre-vote message comprising a pre-vote variable with a first pre-vote value or a second pre-vote value, and comprising a first signature proving the pre-vote and a second signature justifying the pre-vote variable;

(b) once having received $n - t$ valid of the pre-vote messages with pre-vote variables from the participating network devices, performing a main-vote to obtain a main-vote variable

with either a first main-vote value, a second main-vote value, or a third main-vote value, whereby

- if all $n - t$ pre-vote variables have the first pre-vote value then the first main-vote value is obtained, or
- if all $n - t$ pre-vote variables have the second pre-vote value then the second main-vote value is obtained, or
- if the $n - t$ pre-vote variables are different then the third main-vote value is obtained;

(c) broadcasting to the participating network devices a main-vote message comprising the obtained main-vote variable, the first signature and the second signature; and

(d) once having received $n - t$ valid of the main-vote messages, performing a decision,

- if all $n - t$ main-vote variables have the first main-vote value then deciding for the first agree-value or
- if all $n - t$ main-vote variables have the second main-vote value then deciding for the second agree-value,

thereby having achieved the agreement, and helping the other participating network devices to decide; otherwise

(e) broadcasting to the participating network devices a share-value($g^{x_{A,B,C,D}}$) to generate an unpredictable bit $\in$ {Y, N};

(f) receiving at least k share-values ($g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D}$) from the participating network devices, where k is a number larger than t, assembling out of those a common value and deriving one bit thereof; and

(g) repeating the steps starting from a), whereby

- if all $n - t$ main-vote variables have the third main-vote value then the binary value is used as the pre-vote variable, or
- if at least one of all $n - t$ main-vote variables has the first main-vote value then the first pre-vote value is used as the pre-vote variable, or
- if at least one of all $n - t$ main-vote variables has the second main-vote value then the second pre-vote value is used as the pre-vote variable.

20. A computer program product comprising program code means stored on a computer-readable medium for performing the method for achieving agreement among n participating network devices to a first or second agree-value in an asynchronous network, the agreement arising out of a series of messages being sent and received with a signature by each participating network device, whereby the number t of faulty devices is less than $n/3$, each participating network device, said method comprising the steps of :

i) broadcasting to all participating network devices a pre-vote value;

ii) performing a main-vote to amplify majorities if $n - t$ pre-vote values are validly received, and broadcasting to all participating network devices a main-vote value;

iii) deciding for the first or second agree-value based on the received main-vote values, and broadcasting to all participating network devices a share-value to open a cryptographic common coin; and

iv) receiving share-values and assembling out of those a common value, uncovering a bit out of the common value, and repeating the steps starting from i) using the bit as the pre-vote value if the pre-vote values were different.

21. Method for generating an unpredictable bit in an asynchronous network comprising n participating network devices (A, B, C, D), each participating network device performing the following steps:

- providing a secret-value (x_A, x_B, x_C, x_D) and choosing a common number (g) from a cryptographic group (G) corresponding to a linear secret sharing scheme,
  deriving a share-value ($g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D}$) by raising the chosen common number (g) to the power of a monotone function f of the secret-value (x_A, x_B, x_C, x_D);
- broadcasting to the participating network devices (A, B, C, D) the share-value ($g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D}$);
- receiving the share-values ($g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D}$) from the participating network devices (A, B, C, D) and assembling therefrom a common value by combination of at least two of the share-values ($g^{x_A}, g^{x_B}, g^{x_C}, g^{x_D}$) in the exponent of the common number (g); and
- uncovering a binary value of the common value.

22. Method according to claim 21, whereby a two threshold coin is used, where t is the maximum number of traitors in the asynchronous network and k, with $n > k > t$, the number of participating network devices needed to obtain the two threshold coin.

23. Method according to claim 21, whereby the received share-values $(g^{x_B}, g^{x_C}, g^{x_D})$ from the other participating network devices are verified for correctness.